

(19) 日本国特許庁 (J P)

(12) 特 許 公 報 (B 2)

(11) 特許番号

特許第3000968号

(P3000968)

(45) 発行日 平成12年1月17日 (2000.1.17)

(24) 登録日 平成11年11月12日 (1999.11.12)

(51) Int.Cl.<sup>7</sup>

識別記号

F I

H 0 4 L 12/28

H 0 4 L 11/20

D

12/46

11/00

3 1 0 C

請求項の数 2 (全 16 頁)

(21) 出願番号 特願平9-183665

(22) 出願日 平成9年7月9日 (1997.7.9)

(65) 公開番号 特開平11-32047

(43) 公開日 平成11年2月2日 (1999.2.2)

審査請求日 平成9年7月9日 (1997.7.9)

(73) 特許権者 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 森 直樹

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100083987

弁理士 山内 梅雄

審査官 江嶋 清仁

(56) 参考文献 1997信学総大B-7-124

信学論 (B-1) VOL. J80-B-1, NO. 6, P. 366-373

(58) 調査した分野 (Int.Cl.<sup>7</sup>, DB名)

H04L 12/28

H04L 12/46

(54) 【発明の名称】 パケットフィルタリングシステム

1

(57) 【特許請求の範囲】

【請求項1】 非同期転送モードのATMネットワーク上に構築したマルチプロトコルの転送のためのMPOAネットワークで、送信側MPOAクライアントがアドレス解決手順を起動し、受信した受信IPアドレスから出口側のMPOA方式のネットワーク内のクライアントである出口側MPOAクライアントのATMアドレスを獲得するようにした通信システムにおいて、  
アドレス解決要求メッセージを受信してこのメッセージ内の送受信IPアドレスとTCPまたはUDPポート番号をそれぞれ読み込んでこれらをフィルタ用の情報としてのセット情報として、通常のデータ転送のために設定されたフィルタリングの基準に応じてアドレス解決要求に応じるか否かを判定する判定手段と、この判定手段の判定の結果としてアドレス解決要求に応じる場合にはア

2

ドレス解決手順を進行させ、アドレス解決要求に応じない場合にはアドレス解決を中止することで、複数のMPOAサーバ上のフィルタリング基準のすべてに適合するセット情報のパケットに対してのみアドレス解決の結果を返信する返信手段を備えたMPOAサーバと、  
アドレス解決要求メッセージ内に、これから設定するショートカット仮想チャネル・コネクションとしてのショートカットVCCを通して送信するパケットの前記セット情報を挿入する挿入手段と、アドレス解決要求時に前記セット情報のうちアドレス解決が中止されずに完了したもののみを記憶する第1の記憶手段と、パケット送信時にこの第1の記憶手段に記憶した内容と一致するIPパケットのみをショートカットVCCに送信する送信手段と、前記アドレス解決要求時に、前記MPOAサーバから通知されたショートカットVCCを通して送信され

10

## 3

てくるパケットの前記セット情報を記憶する第2の記憶手段と、パケット受信時にこの第2の記憶手段に記憶したセット情報と一致するIPパケットのみをショートカットVCCから受けて、これ以外のIPパケットは廃棄するパケットフィルタリング手段とを備えたMPOAクライアントとを具備することを特徴とするパケットフィルタリングシステム。

【請求項2】 ATMインタフェースと他のネットワークインタフェースを持ったデバイスとしてのエッジデバイスやATM端末がトランスポート・コントロール・プロトコル/ユーザ・データグラム・プロトコルとしてのTCP/UDPヘッダとIPヘッダを読むことで、前記セット情報によるパケットフィルタリングを実現することを特徴とする請求項1記載のパケットフィルタリングシステム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は非同期転送ネットワークを使用したTCP/IPプロトコルによるインターネットに係わり、特にインターネットでセキュリティ機能を実現するために許可されたデータのみを通過させるためのパケットフィルタリングシステムに関する。

## 【0002】

【従来の技術】ネットワーク層にIP(Internet Protocol)を使用し、トランスポート層にTCP(Transport Control Protocol)を使用してTCP/IP(Transport Control Protocol/Internet Protocol)ネットワークを相互接続するために、ルータが従来から使用されている。ルータは複数のネットワークインタフェースを有しており、ネットワーク層までの処理を終端する。また、トランスポート層の処理も一部行うことがある。

【0003】このルータの機能の1つとして、パケットの選択的通過すなわちフィルタリングによる通信のセキュリティの確保がある。今、あるネットワークの外部に存在するIPノードが、そのネットワークの内部に存在するIPノードと通信を行うものとする。このとき、パケットはそのネットワークの出入口に配置されたルータを経由する。ルータは、その通過しようとするパケット内のネットワーク層とトランスポート層のヘッダを読んで転送処理を行う。このため、通過してよいIPパケットの送信ノードおよび受信ノードのIPアドレスとTCP/UDP(Transport Control Protocol/User Datagram Protocol)のポート番号(セット情報)を予め設定しておいて、これと照合して該当しないパケットを廃棄するように設定しておけば、アクセスを制限することができる。すなわち、ネットワーク内部のIPノードを外部からアクセスできないようにしたり、トランスポート層の特定のポートへのアクセスを禁止したりすることが可能になる。これらは、それぞれ、ネットワーク層レベルにおけるパケットフィルタリングあるいはトランスポ

## 4

ート層レベルのパケットフィルタリングと呼ばれており、通信のセキュリティを高めることに有効である。

【0004】一方、ネットワークの高速化を図るために、ルータの代わりに高速なATM(Asynchronous Transfer Mode: 非同期転送モード)交換機を使用してTCP/IPネットワークを構築するための技術が開発されている。例えば、OSI(OpenSystems Interconnection: 開放型システム間相互接続)階層モデルでの第2層以下にATMを使用し、第3および第4層にTCP/IPプロトコルを使用するときの通信方式が、ATM・フォーラム(The ATM Forum)等で審議されており、“ATM Forum 96-0824r9”等の仕様書が発表されている。

“ATM Forum 96-0824r9”の仕様はMPOA(Multiprotocol over ATM: マルチプロトコルを転送する仕組み)方式と呼ばれており、ATMネットワークインタフェースを持った端末やネットワークデバイスをMPOAクライアント(MPC)とし、ルータ機能を有する装置をMPOAサーバ(MPS)としてネットワークを構成する。

【0005】MPCがMACフレームを転送するとき、送り先が同一サブネット内のMPCまたはそのMPCに収容される端末である場合には、ATM・フォーラムが規定しているLAN(Local Area Network: 企業情報通信網)エミュレーション(LANE)プロトコルを用いて通信を行う。送り先が異なるサブネット内にあり、MPS(MPOA方式のネットワーク内のサーバ)機能を持つルータにMAC(Media Access Control: 媒体アクセス制御)フレーム内のIPアドレスを読み、そのIPアドレスごとにパケットをカウントするようにしている。得られたカウント値が単位時間内に一定値以下であれば、前記したMPSにMACフレームを送信し、MPSは従来のルータと同じ動作で、IPパケットを宛先のIPアドレスのノードまで送るようにする。

【0006】これに対してカウント値が単位時間内に前記した一定値を越えた場合には、前記したMPSにMACフレームを送信する代わりに、宛先IPアドレスのノードと同一サブネットに存在するMPCまでVCC(Virtual Channel Connection: 仮想チャネル・コネクション)を設定し、そのVCCを通してパケットを送る。これにより、ルータ(MPS)をショートカットして、ATMの入口側のMPCから、出口側のMPCにIPパケットを送信することができる。したがって、前記したVCCは、ショートカットVCCと呼ばれている。ここでATMの入口側とは、他のネットワークからMPOA(Multiprotocol Over ATM: ATM上でマルチプロトコルを転送する仕組み)ネットワークにデータが流入するノードを表わしており、出口側とは、MPOAネットワークから他のネットワークにデータが流出するノードを表わしている。

【0007】ショートカットVCCを設定するには、入

口側のMPCがパケット内の受信先のIPアドレスから、出口側のMPCのATMアドレスを得ることが必要である。このため、入口側MPCは、MPOAレゾリューション・リクエスト(Resolution Request)を、同一サブネット内のMPSに送出する。そして、MPSが出口側MPCと同じサブネットのときには、入口側MPCに対してMPOAレゾリューション・リプライ(Resolution Reply)で知らせ、出口側MPCに対してはMPOAインポジション・リクエスト(Imposition Request)を送る。また、ショートカットVCCを通して送られてくるMACフレームを、出口側のMPSから送られてきたように見せるために、出口側MPCでレイヤ2の情報を載せてMACフレームを送出する必要がある。このため、出口側MPSから出口側MPCに前記したMPOAインポジション・リクエスト・メッセージで通知を行う。MPSが出口側MPCとは異なるサブネットにあるときには、次段のMPSにMPOAレゾリューション・リクエスト・メッセージを送ることになる。

【0008】以上説明した手順で、入口側MPCが出口側のMPCのATMアドレスを獲得したら、標準のATMのシグナリング手順(ATM Forum UNI3.1 またはITU-TQ. 2931)を用いて、入口側MPCと出口側MPCの間にショートカットVCCを設定する。そして以後、出口側MPCに送出する必要があるデータは、このショートカットVCCを通して送信することになっている。これにより、MPSにパケットを送信するよりも高速なデータ転送が可能になる。

#### 【0009】

【発明が解決しようとする課題】以上説明したようなMPOA方式では、ショートカットVCCを用いて送信されるTCP/UDPパケットが入口側MPCで48バイトのセルに分割されてネットワークに送られる。そして、中継ATM交換機をセルのままでスイッチングされて、出口側MPCで再びTCP/UDPパケットに組み立てられる。このため、ルータを使用した場合と異なっており、中継のATM交換機はパケット内のTCP/UDPヘッダやIPヘッダの読み込みを行わない。したがって、ATM交換機を使用した場合には、ルータが従来行っていたトランスポート層レベルやネットワーク層レベルでのパケットのフィルタリングが不可能になるという問題があった。

【0010】そこで本発明の目的は、MPOA方式のネットワークで、ルータと同様のパケットフィルタリング機能を実現することのできるパケットフィルタリングシステムを提供することにある。

#### 【0011】

【課題を解決するための手段】請求項1記載の発明では、非同期転送モードのATMネットワーク上に構築したマルチプロトコルの転送のためのMPOAネットワークで、送信側MPOAクライアントがアドレス解決手順

を起動し、受信した受信IPアドレスから出口側のMPOA方式のネットワーク内のクライアントである出口側MPOAクライアントのATMアドレスを獲得するようにした通信システムにおいて、(イ)アドレス解決要求メッセージを受信してこのメッセージ内の送受信IPアドレスとTCPまたはUDPポート番号をそれぞれ読み込んでこれらをフィルタ用の情報としてのセット情報として、通常のデータ転送のために設定されたフィルタリングの基準に応じてアドレス解決要求に応じるか否かを判定する判定手段と、この判定手段の判定の結果としてアドレス解決要求に応じる場合にはアドレス解決手順を進行させ、アドレス解決要求に応じない場合にはアドレス解決を中止することで、複数のMPOAサーバ上のフィルタリング基準のすべてに適合するセット情報のパケットに対してのみアドレス解決の結果を返信する返信手段を備えたMPOAサーバと、(ロ)アドレス解決要求メッセージ内に、これから設定するショートカット仮想チャネル・コネクションとしてのショートカットVCCを通して送信するパケットのセット情報を挿入する挿入手段と、アドレス解決要求時にセット情報のうちアドレス解決が中止されずに完了したもののみを記憶する第1の記憶手段と、パケット送信時にこの第1の記憶手段に記憶した内容と一致するIPパケットのみをショートカットVCCに送信する送信手段と、アドレス解決要求時に、MPOAサーバから通知されたショートカットVCCを通して送信されてくるパケットのセット情報を記憶する第2の記憶手段と、パケット受信時にこの第2の記憶手段に記憶したセット情報と一致するIPパケットのみをショートカットVCCから受けて、これ以外のIPパケットは廃棄するパケットフィルタリング手段とを備えたMPOAクライアントとをパケットフィルタリングシステムに具備させる。

#### 【0012】

【0013】また、請求項2記載の発明では、ATMインタフェースと他のネットワークインタフェースを持ったデバイスとしてのエッジデバイスやATM端末がトランスポート・コントロール・プロトコル/ユーザ・データグラム・プロトコルとしてのTCP/UDPヘッダとIPヘッダを読むことで、IPアドレスとTCP/UDPポート番号によるパケットフィルタリングを実現することを特徴としている。

【0014】すなわち本発明のパケットフィルタリングシステムでは、従来のルータと同様に、MPSにトランスポートレイヤとネットワークレイヤの情報によるフィルタリング規則を基にした基準を記述しておく。そして、入口側MPCが、ATM交換機を用いたネットワーク上でTCP/IPプロトコルによって通信を行う手法としてのMPOAプロトコルを使用して出口側MPCのATMアドレスを解決するときに、送信されるパケットの送信・受信ノードのIPアドレスと、トランスポート

層プロトコル(TCPまたはUDP)と、TCP/UDPポート番号を申告し、それらが前記した基準によって禁止されていないかを中継のMPSで検査する。この結果として禁止されていない場合には、アドレス解決手順が進められるが、禁止されていればアドレス解決手順を中止し、ショートカットVCCを設定させないようにして、VCC設定時のフィルタリングを実現する。

【0015】これに加えて、VCCの設定後では、前記した入口側MPCがアドレス解決要求時に申告した属性を有するTCP/IPパケットのみを送信し、それ以外のパケットはショートカットVCCに送信しないようにして、データ送信時のフィルタリングを実現する。前記した出口側MPCでは、アドレス解決要求時に、入口側MPCから入口側MPSを通して申告された属性を有するTCP/IPパケットのみを受け取り、それ以外のパケットを廃棄する。これにより、データ受信時のフィルタリングが実現される。

【0016】

【発明の実施の形態】

【0017】

【実施例】以下実施例につき本発明を詳細に説明する。

【0018】本実施例のパケットフィルタリングシステムでは、異なるサブネットにあるMPC間でIPパケット通信を行うときに、IPパケットのヘッダ内の送信・受信ノードのIPアドレスと、TCP/UDPポート番号の双方によってフィルタリングを行うようにしている。MPCは、ATMインタフェースを持った端末の場合と、ATMインタフェースと他のネットワークインタフェースを持ったデバイス(これをエッジデバイスという。)の場合とがある。本実施例では後者のエッジデバイスの場合について説明を行う。また、実施例ではIPパケットヘッダ内の受信ノードのIPアドレスまたはTCP/UDPポート番号が異なるパケットでも、同一の入口側MPCと出口側MPCをとるパケットは、同一のショートカットVCCを使用する構成となっている。

【0019】図1は本発明の一実施例におけるエッジデバイスの機能的な構成を表わしたものである。このエッジデバイスで、LEC(LAN Emulation Client)処理部11は、LANEL(LAN Emulation)プロトコルを用いて、同一サブネット内のLECにMACフレームを転送するための処理を行う。LEC処理部11と接続されたMPC処理部12は、MPOAプロトコルを使用して、IPパケットをカプセル化したMACフレームをMPSと送受信したり、他のサブネット内のMPCへのショートカットVCCの設定のためのアドレス解決手順を行う。

【0020】LEC処理部11およびMPC処理部12に接続されたVC(Virtual Circuit)テーブル13は、設定したATMのVCCについての登録および管理を行う。ATM VC終端部14は、図示しないATM

ネットワークとのインタフェースであり、ATMセルからパケットへの組み立てと、パケットからATMセルへの分解を行うようになっている。MPC処理部12に接続された非ATMネットワークインタフェース15は、ATM以外のネットワークとの入出力インタフェース部である。

【0021】VCテーブル13およびATM VC終端部14と接続されたATMシグナリング処理部16は、ATM VCCを設定するためのシグナリングの制御と処理を行うようになっている。MPC処理部12と接続されたショートカットVCCテーブル17は、MPOAプロトコルとATMシグナリングを用いて設定したショートカットVCC用のテーブルである。このショートカットVCCテーブル17の各ショートカットVCCエントリには、そこを通過して送受信してもよいTCP/IPパケットの属性が書かれるようになっている。

【0022】図2は入口側MPCでのショートカットVCCテーブルの例を示しており、図3は出口側MPCでのショートカットVCCテーブルの例を示している。

【0023】図4は、MPSの機能的な構成を表わしたものである。LEC(LAN Emulation Client)処理部21は、LANE(LAN Emulation)プロトコルを用いて、同一サブネット内のLECと通信を行う部分である。このLEC処理部21と接続されたMPS処理部22は、MPOAプロトコルに基づいて、入力側MPCと出口側MPCに対してショートカットVCCを設定するためのアドレス解決手順を制御する部分である。ルータ機能部23は、他のMPSや同一ネットワーク内のMPCから送信されてきたIPパケットを、別のMPSや他のサブネット内のMPCに転送するためのルータとしての処理を行う。LEC処理部21、MPS処理部22およびルータ機能部23と接続されたVCテーブル24は、設定したATMのVCCの登録や管理を行うようになっている。このVCテーブル24に接続されたATM VC終端部25は、図示しないATMネットワークとのインタフェースであり、ATMセルからパケットへの組み立てや、パケットからATMセルへの分解を行うようになっている。

【0024】VCテーブル24およびATM VC終端部25に接続されたATMシグナリング処理部26は、ATM VCCを設定するためのシグナリングの制御と処理を行う。MPS処理部22およびルータ機能部23と接続されたルーティング部27は、他のサブネット内のMPCやMPSを探すためのルート検索テーブルである。このルート検索テーブルは、ルーティングプロトコルで動的に設定される場合と、管理者により静的に設定される場合とがある。ルート検索テーブル27に接続されたMPSパケットフィルタリング機能28は、そのMPSを通したMPOAプロトコルによるアドレス解決に制限を加え、ショートカットVCCの設定を制限する部

分であり、管理者がこれを予め設定する。

【0025】図5は、MPSパケットフィルタリング機能部の一例を示したものである。この図で列“1”は、IPアドレスが“111.111.22.22”である送信端末のTCP“8010”番ポートと、IPアドレスが“112.112.12.12”である受信端末のTCPの25番から100番までのポートとの間に、ショートカットVCCを設定してもよいことを示す。列“2”は、IPアドレスが“122.122.22.\*”であるネットワークに存在する送信端末のUDP (User Datagram Protocol) “517”番ポートを使用するアプリケーションAP-1と、IPアドレスが“122.112.12.\*”のネットワークに存在する受信端末のUDP“8080”番ポートを使用するアプリケーションAP-1との間に、ショートカットVCCを設定してもよいことを示す。

【0026】この図5に示すように、送信IPアドレス（またはそのプレフィックス）と受信IPアドレス（またはそのプレフィックス）の組で1つのエントリが構成され、かつここでアドレスの解決が禁止されていない場合のみ、アドレス解決未処理の回答要求を行うようになっている。

【0027】図6は、入口側MPCが、ATM以外のネットワークから受けたMACフレームを中継するときの処理の流れを表わしたものである。まず、入口側MPCは、受信したMACフレーム内の受信先MACアドレスと受信先IPアドレスを読み出す（ステップS101）。そして、受信先MACアドレスが同一サブネット内のMPSであるか否かを判別する（ステップS102）。受信先MACアドレスが同一サブネット内のMPS以外である場合には（Y）、LANEプロトコルを用いて、受信先のノードにMACフレームを送る（ステップS103）。

【0028】これに対して、受信先MACアドレスが同一サブネット内のMPSである場合（ステップS102：N）、受信先IPアドレスを鍵として、ショートカットVCCテーブル17内のショートカットVCCのエントリを検索する（ステップS104）。この鍵に対するエントリが見つからない場合には（ステップS105：N）、新たにエントリを作成し、そのカウンタのカウント値を“1”に設定して、受信したMACフレームを入口側MPSに送る（ステップS106）。この鍵に対応するエントリが見つかった場合には（ステップS105：Y）、ショートカットVCCが未設定であるかどうかを判別する（ステップS107）。

【0029】図7は、鍵に対応するエントリが見つかったがそのショートカットVCCが未設定の場合の処理手順を表わしたものである。この場合には、まずカウント値を“1”加算する（ステップS201）。そして、ショートカットVCCエントリのカウント値とあらかじめ

設定されたしきい値とを比較する（ステップS202）。この結果、しきい値の方が大きいときには（ステップS203：Y）、入口側MPSにMACフレームを送信して処理を終える（エンド）。カウント値の方が大きいか両者が等しい場合には、MACフレームの中のIPパケットヘッダ内の送受信IPアドレスと、TCP/UDPポート番号を読み、そのパケットを入口側MPSに送る（ステップS204）。次に、出口側MPCのATMアドレスを得るために、MPOAレゾリューション・リクエスト・メッセージを同一サブネット内のMPS（入口側MPS）に送信する（ステップS205）。このメッセージに、標準のMPOAプロトコルで規定される情報を加えて、ステップS204で読み出したIPパケットの送受信IPアドレスとTCP/UDPポート番号を含める。このMPOAレゾリューション・リクエストが成功すると、次の手順として入口側MPSからMPOAレゾリューション・リプライが戻り、出口側MPCのATMアドレスが通知される（ステップS206）。

【0030】次に、前記したエントリに、出口側MPCのATMアドレスと、送信するTCP/IPパケットの送信・受信IPアドレスと、TCP/UDPポート番号を登録する（ステップS207）。そして、出口側MPCのATMアドレスを宛先として、標準のATMシグナリング手順を行って、ショートカットVCCを設定する（ステップS208）。その後、ステップS208で設定したショートカットVCCのVPI/VC（Virtual Path identifier / Virtual Channel identifier；仮想パス識別子／仮想チャネル識別子）を、前記したショートカットVCCのエントリに設定する（ステップS209）。

【0031】図8は、図6のステップS107で鍵に対応するエントリが見つかり、ショートカットVCCが設定済である場合の処理の流れを表わしたものである。この場合には、まずMACフレーム中のIPパケットヘッダの送信・受信IPアドレスとTCP/UDPポート番号を読み出す（ステップS301）。そして、出口側MPCへのショートカットVCCが設定されているので、この設定されているショートカットVCCエントリ中の送信・受信IPアドレスおよびTCP/UDPポート番号を、ステップS301で読んだIPパケット内の送信・受信IPアドレスおよびTCP/UDPポート番号とそれぞれ比較する（ステップS302）。これらの値がどれも一致している場合には（ステップS303：Y）、前記したエントリの出口側MPCへのショートカットVCCに、受信したMACフレームを送信する（ステップS304）。

【0032】これらの値のいずれかが等しくない場合には（ステップS303：N）、入口側のMPSに対してMPOAレゾリューション・リクエストを送信し、受信したMACフレームを入口側MPSに送る（ステップS3

05)。このメッセージに、標準のMPOAプロトコルで規定される所と共に、ステップS301で読み出したIPパケットの送受信IPアドレスとTCP/UDPポート番号とを含める。このMPOAレゾリューション・リクエストが成功して、MPSからMPOAレゾリューション・リプライが戻ってきた場合には(ステップS306:Y)、出口側MPCのATMアドレスが通知され、前記したIPパケットの送信が許可されたことになる。したがって、このときには、前記したエントリに、新たに送信するTCP/IPパケットの送信・受信アドレスと、TCP/UDPポート番号を追加登録する(ステップS307)。

【0033】ステップS306でMPSからMPOAレゾリューション・リプライが戻ってこない場合には

(N)、前記したIPパケットをショートカットVCCを通して送信することが許可されないことになり、処理を終える(エンド)。

【0034】図9は、MPSが、入口側のMPCからMPOAレゾリューション・リクエスト・メッセージを受けるときの処理の流れを表わしたものである。まず図4に示したMPS処理部22は、隣接したMPCからMPOAレゾリューション・リクエスト・メッセージを受信する(ステップS401)。次に、そのメッセージ中の送信・受信IPアドレスとTCP/UDPポート番号を読む(ステップS402)。そして、MPSパケットフィルタリング機能部28(図4)を検索して、そのパケットをショートカットVCCを通して受信するために、アドレス解決をしてよいかの判定処理を行う(ステップS403)。この結果、解決が許可されていない時には(ステップS404:Y)、そのMPOAレゾリューション・リクエスト・メッセージを廃棄し、入力側MPCと出力側MPCにショートカットVCCを設定するのを中断させる(ステップS405)。

【0035】これに対して、ステップS404で解決が許可されているときには(N)、受信先IPアドレスから、ルーティング部27を用いて、出口側MPCへのルートを検索する(ステップS406)。出口側MPCがこのMPSと異なるサブネットに存在する時には、(ステップS407:Y)、次段のNHRP(Next Hop Resolution Protocol)サーバに前記したMPOAレゾリューション・リクエスト・メッセージを転送する(ステップS408)。ステップS407で出口側MPCが同一サブネットに存在するときには(N)、出口側MPCに対して、MPOAキャッシュ・インポジション(Cache Impo-  
sition)・メッセージを送信する(ステップS409)。このメッセージの中には、標準のMPOAプロトコルで規定されている、このMPSのMACアドレスと、受信先のIPノードのMACアドレスおよび受信先のIPアドレスに加えて、そのショートカットVCCを通して送られるパケットの送信IPアドレスと送受信の

TCP/UDPポート番号とが含まれる。次に入口側MPCに対して、MPOAレゾリューション・リプライ(Resolution Reply)メッセージを送る。

【0036】図10は、MPCが、ショートカットVCCを設定するために、出口側MPSからMPOAキャッシュ・インポジション・メッセージを受信する場合の処理の流れを表わしたものである。まず、MPOAキャッシュ・インポジション・メッセージを受信する(ステップS501)。次にこのMPOAキャッシュ・インポジション・メッセージから、標準のMPOAプロトコルで規定されている入口側MPCのATMアドレスと、出口側MPSのMACアドレスと、受信IPノードのMACアドレスに加えて、送信されるIPパケットの受信IPアドレスと、送受信のTCP/UDPポート番号を読み取る(ステップS502)。

【0037】次に、入口側MPCのATMアドレスと、受信IPノードのIPアドレスを鍵として、ショートカットVCCテーブル17(図1)にエントリを検索する(ステップS503)。エントリがない場合には(ステップS504:Y)、ステップS502で読み出した、送信されるTCP/IPパケットの送受信IPアドレスと、TCP/UDPポート番号と、入口側MPCのATMアドレスと、出口側MPSのMACアドレスおよび受信IPノードのMACアドレスを、ショートカットVCCテーブル17に登録する(ステップS505)。その後、ATMシグナリング手順によってショートカットVCCのVPI/VCIが決定されるので、その値を前記したエントリに登録する(ステップS506)。

【0038】ステップS504でエントリが既に存在する場合には、ステップS502で読み出した、送信されるパケットの送信IPアドレスと、送信・受信TCP/UDPポート番号をこのエントリに追加登録する(ステップS506)。

【0039】図11は、出口側MPCが、ショートカットVCCを通してパケットを受信するときの処理の流れを表わしたものである。まず、ショートカットVCCを通して、セル化されたIPパケットを受信する(ステップS601)。次に、図1に示したATM VC終端部14でセルからIPパケットを組み立てる(ステップS602)。そして、出口側ショートカットVCCテーブル17(図1)内で、パケットが送られてきたショートカットVCCのVPI/VCIと受信先IPアドレスを鍵として、該当するエントリを検索する(ステップS603)。次に、受信したいIPパケット内の送信・受信IPアドレスとTCP/UDPポート番号を読み出す(ステップS604)。そして、ステップS604で読んだ値と前記したショートカットVCCの該当エントリの送信・受信IPアドレスとTCP/UDPポート番号とを比較する(ステップS605)。

【0040】この結果としていずれも等しいときには

10

20

30

40

50

(ステップS606:Y)、許可されたパケットであるとして、同一サブネット内のMPSのMACアドレスと、受信先のIPノードのMACアドレスを付加してMACフレームとし、非ATMインターフェース15(図1)から該当するネットワークに送信する(ステップS607)。ステップS606でいずれかが等しくない場合には(N)、違反パケットであるとみなしてこれを廃棄し、パケットフィルタリングを実行することになる(ステップS608)。

#### 【0041】

【発明の効果】以上説明したように請求項1～請求項2記載の発明によれば、TCP/UDPパケットごとにATM交換機でTCP/UDPヘッダとIPヘッダを読まなくとも、エッジデバイスやATM端末でそれらのヘッダを読むことで、IPアドレスとTCP/UDPポート番号によるパケットフィルタリングを実現することができる。本発明では、あらかじめフィルタリングの基準を設定しておくので、たとえば、これをMPS機能を持ったルータで設定した実施例の図5で示したような基準とすれば、これがMPOAプロトコルのメッセージと共に、エッジデバイスやATM端末に伝播する。したがって、MPS機能を持ったルータに適切なフィルタリング規則の内容を設定しておく、その下流側に存在するすべてのIPノードの通信の安全性が向上するという利点がある。しかも本発明では、単にフィルタ条件を判定してその結果がクライアントに返されるのではなく、それぞれのサーバを通過可能などときにはこれらによるアドレス解決手順が続行されるので、フィルタ条件を重畳させた形でクライアントが取得するという効果がある。

#### 【図面の簡単な説明】

【図1】本発明の一実施例におけるエッジデバイスの機能的な構成を示すブロック図である。

【図2】本実施例の入口側MPCでのショートカットVCCテーブルの内容を示した説明図である。

【図3】本実施例の出口側MPCでのショートカットV

CCテーブルの内容を示した説明図である。

【図4】本実施例のMPSの機能的な構成を表わしたブロック図である。

【図5】MPSパケットフィルタリング機能部の一例を示した説明図である。

【図6】入口側MPCが、ATM以外のネットワークから受けたMACフレームを中継するときの処理の流れを表わした流れ図である。

10 【図7】鍵に対応するエントリが見つかったがそのショートカットVCCが未設定の場合の処理手順を表わした流れ図である。

【図8】図6のステップS107で鍵に対応するエントリが見つかり、ショートカットVCCが設定済である場合の処理の流れを表わした流れ図である。

【図9】MPSが、入口側のMPCからMPOAレゾリューション・リクエスト・メッセージを受けるときの処理の流れを表わした流れ図である。

20 【図10】MPCが、ショートカットVCCを設定するために、出口側MPSからMPOAキャッシュ・インポジション・メッセージを受信する場合の処理の流れを表わした流れ図である。

【図11】出口側MPCが、ショートカットVCCを通してパケットを受信するときの処理の流れを表わした流れ図である。

#### 【符号の説明】

11、21 LEC処理部

12 MPC処理部

13、22、24 VCテーブル

14、25 ATM VC終端部

30 15 非ATMネットワークインターフェース部

16、26 ATMシグナリング処理部

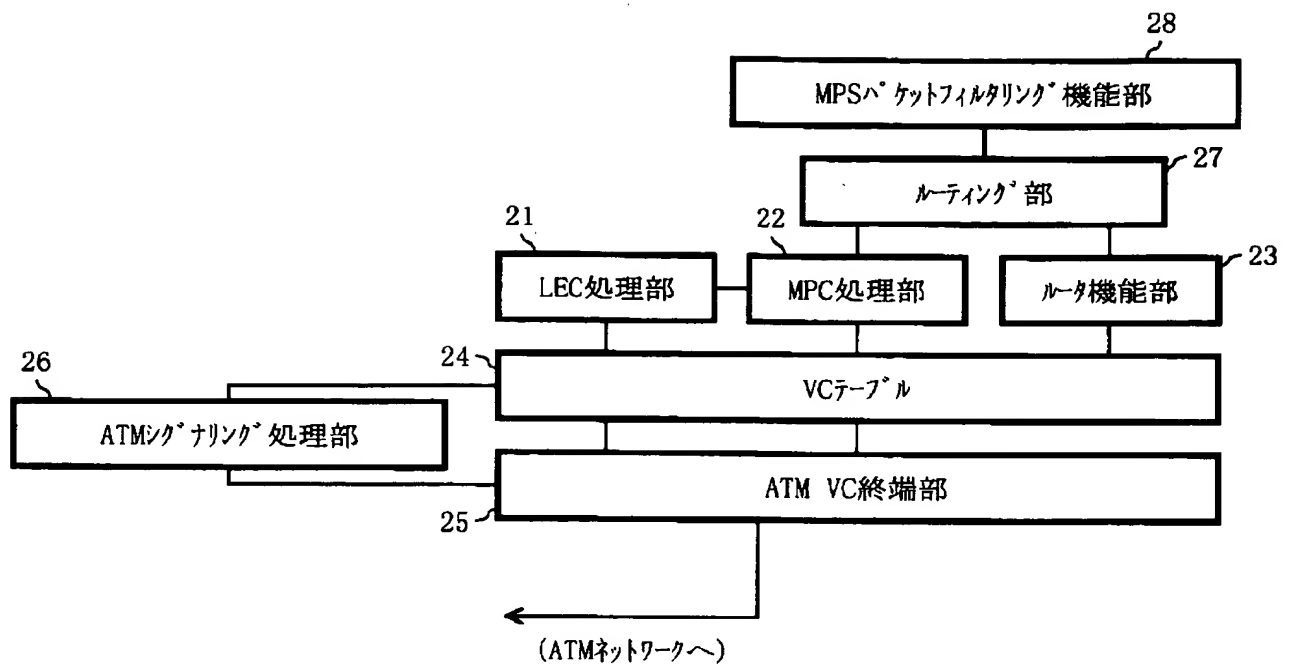
17 ショートカットVCCテーブル

23 ルータ機能部

27 ルーティング部

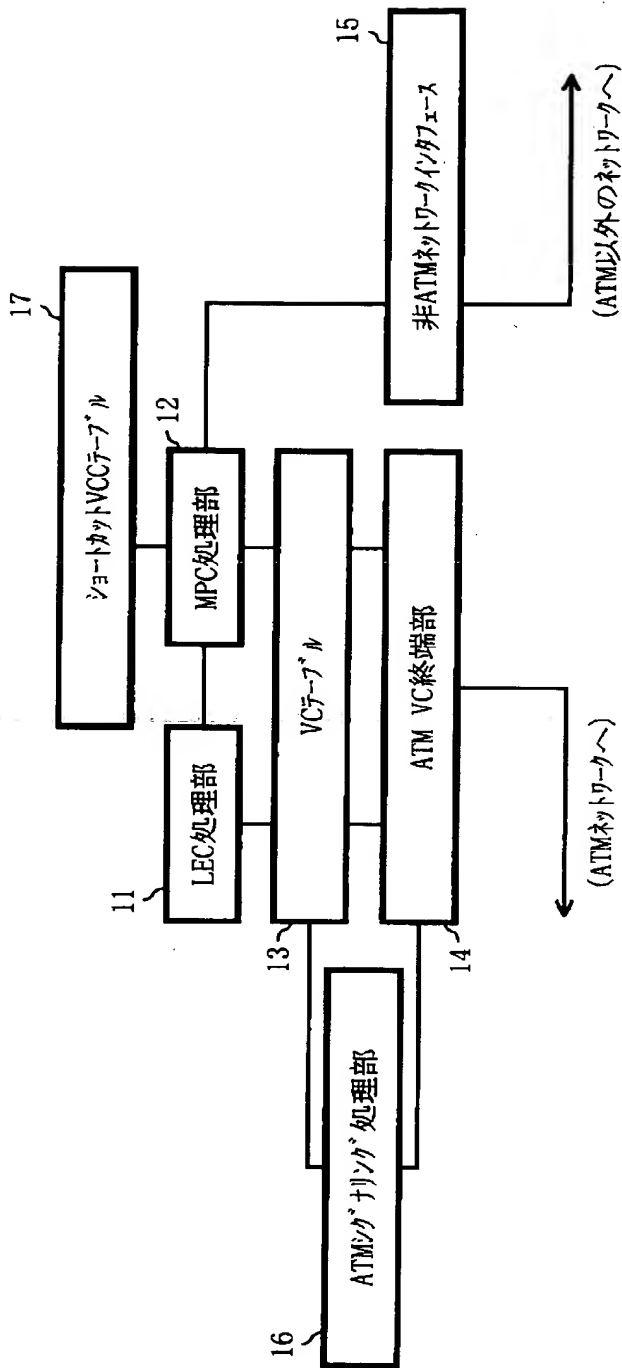
28 MPSパケットフィルタリング機能部

【図4】





【図1】



【図2】

| 鍵     |           | 内容       |      |                            |
|-------|-----------|----------|------|----------------------------|
| LEC番号 | 受信MACアドレス | 受信IPアドレス | カウンタ | 受信ATMアドレス                  |
|       |           |          |      | VPI/VCI                    |
|       |           |          |      | 送受信IPアドレス, TCP/UDPポート番号リスト |

【図3】

| 鍵         |         |          | 内容                         |
|-----------|---------|----------|----------------------------|
| 送信ATMアドレス | VPI/VCI | 受信IPアドレス | 送信MACアドレス                  |
|           |         | LEC      | 送受信IPアドレス, TCP/UDPポート番号リスト |

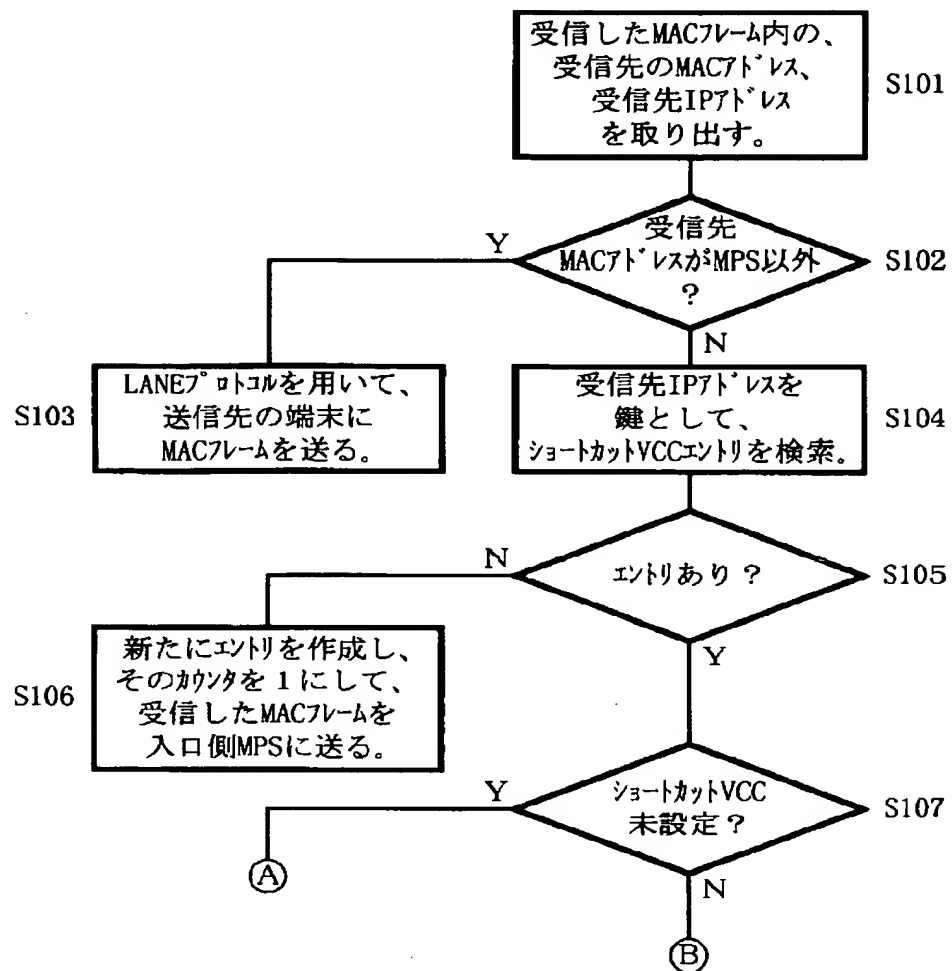
【図5】

| 送信端末の<br>IPアドレス | 送信端末の<br>TCP/UDPポート番号 | 受信端末の<br>IPアドレス | 受信端末の<br>TCP/UDPポート番号 | アプリケーション<br>識別子 |
|-----------------|-----------------------|-----------------|-----------------------|-----------------|
| 111.111.22.22   | 8010/TCP              | 112.112.12.112  | 25-100/TCP            | 指定なし            |
| 122.122.22*     | 517/UDP               | 122.112.12*     | 8080/UDP              | AP-1/AP-1       |

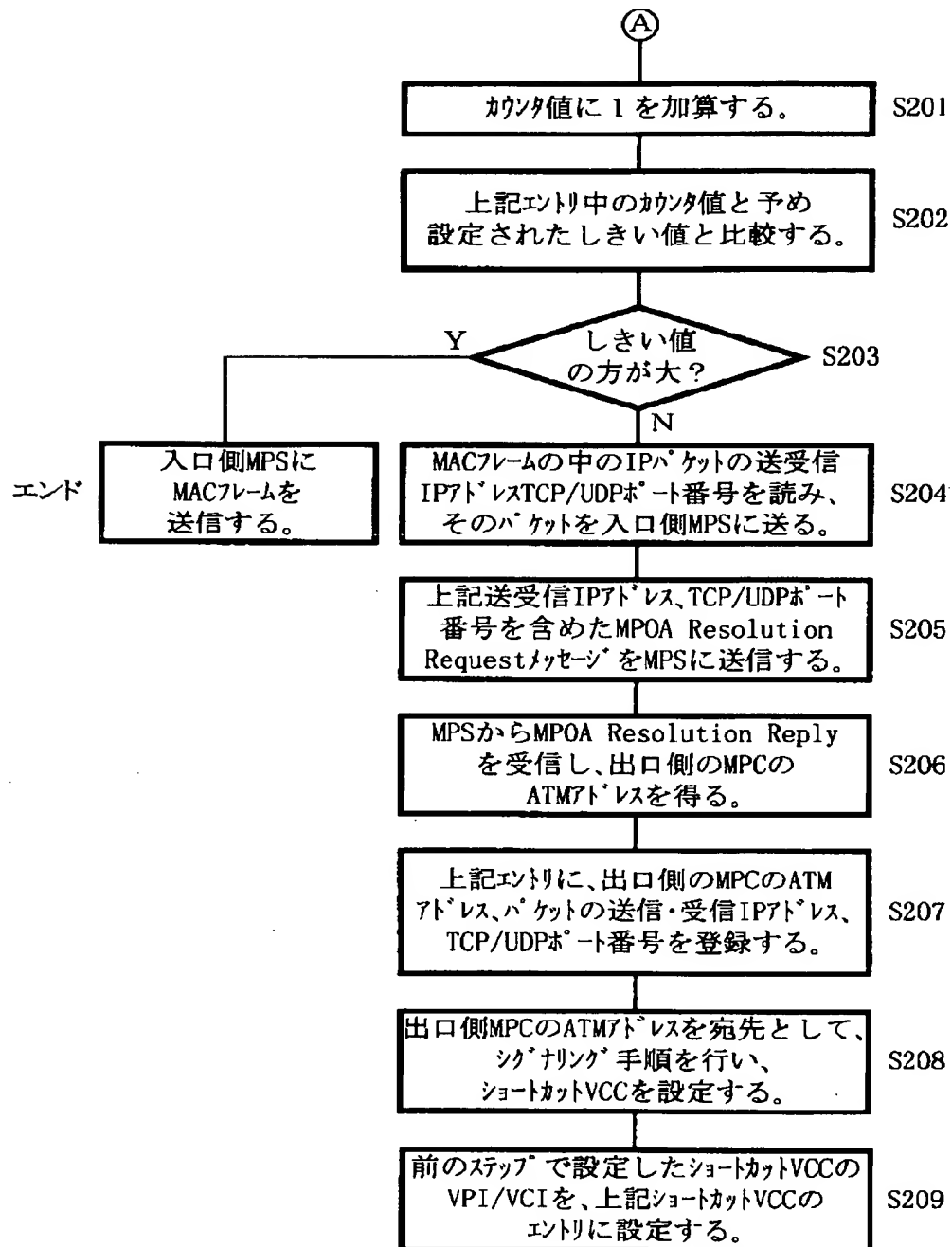
列“1”

列“2”

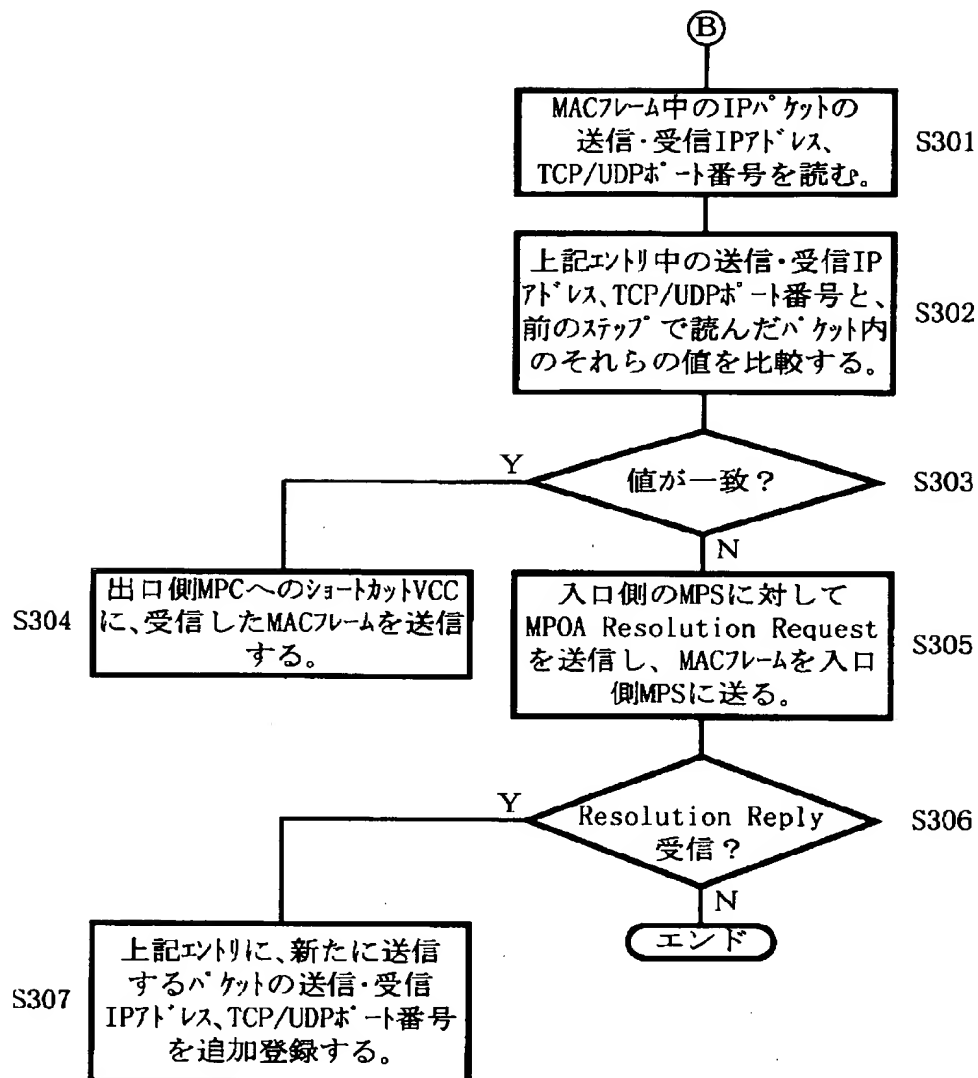
【図6】



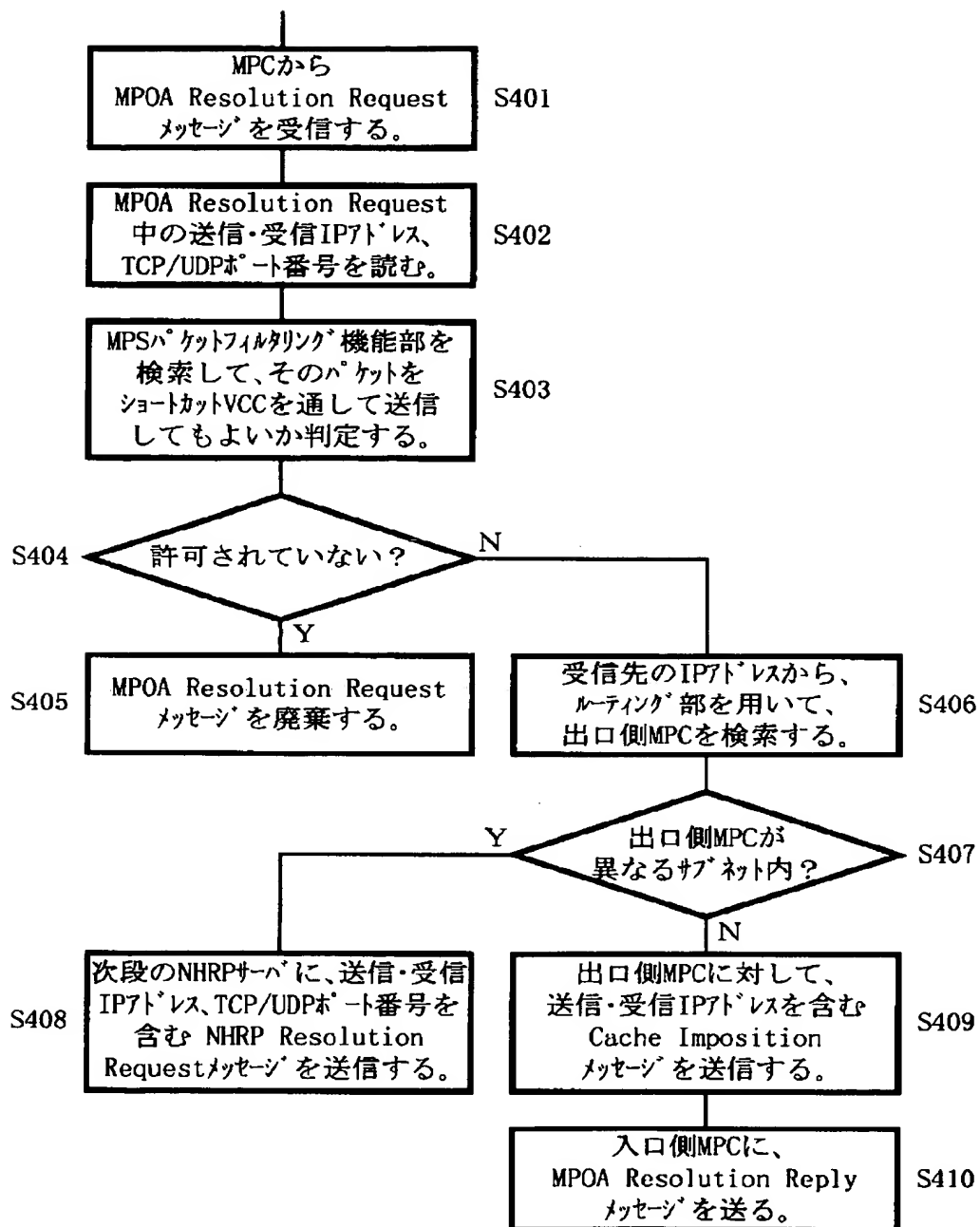
【図7】



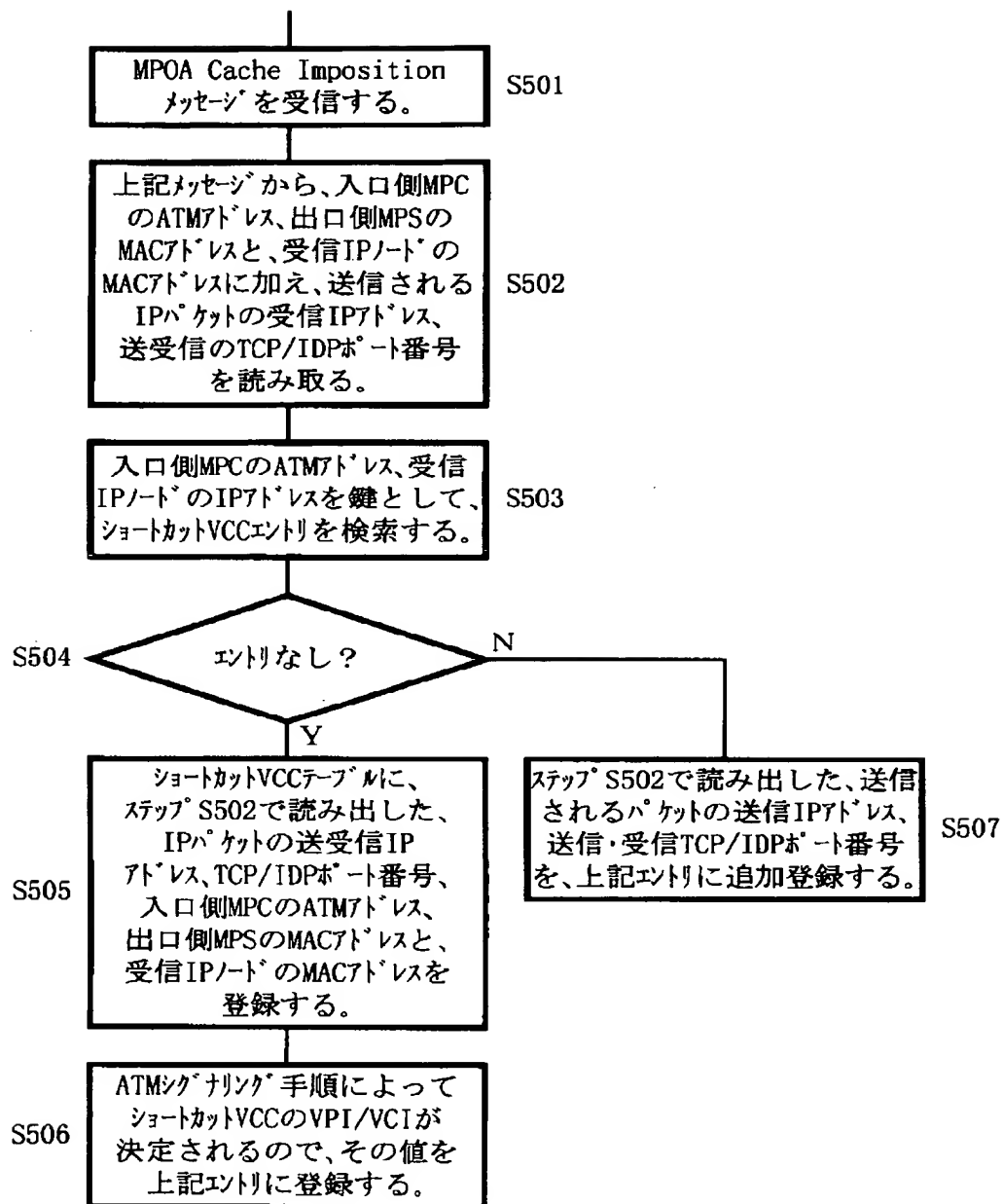
【図8】



【図9】



【図10】



【図11】

